

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10,789,311	§	
Filed:	February 27, 2004	§	Examiner: Unknown
Inventor(s):		§	Group/Art Unit: 2124
Hans Eberle		§	Atty. Dkt. No: 6000-31500
Nils Gura		§	
Lawrence Spracklen		§	
Sheueling Chang-Shantz		§	
Leonard Rarick		§	
Title:	Method and Apparatus for	§	
	Implementing Processor	§	
	Instructions for	§	
	Accelerating Public-Key	§	
	Cryptography	§	

TRANSMITTAL OF POWER OF ATTORNEY AND
NOTICE OF CHANGE OF ADDRESS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Please find attached a Power of Attorney with regard to the above-identified patent application. Applicant respectfully requests the Commissioner to change the correspondence address for the above-identified patent application. The old correspondence address was:

Mark Zagorin
Zagorin, O'Brien & Graham, L.L.P.
7600B N. Capital of Texas Hwy, Suite 350
Austin, Texas 78731

The new correspondence address is:

Robert C. Kowert
Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, Texas 78767-0398
(512) 853-8850

If there are any questions regarding this matter, please contact me at the telephone number provided below.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicant(s)

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, Texas 78767-0398
(512) 853-8850

Date: February 13, 2007

POWER OF ATTORNEY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

SUN MICROSYSTEMS, INC., ("assignee"), a Delaware corporation having a place of business at 4150 Network Circle, Santa Clara, California 95054, certifies that to the best of assignee's knowledge and belief it is the assignee of the entire right, title, and interest in and to the applications listed in Appendix A (attached hereto) and represents that the undersigned is a representative authorized and empowered to sign on behalf of the assignee.

Assignee has reviewed the assignment documents that evidence the placement of title in the assignee, true and correct copies of which are attached hereto, and understands and believes that these assignment documents have been submitted for recordation in the U.S. Patent and Trademark Office.

Pursuant to 37 C.F.R. §§1.36 and 3.71, the assignee hereby revokes all powers of attorney previously given and appoints

I hereby revoke any previous Powers of Attorney and appoint the practitioners at Customer Number 58467.

Pursuant to 37 C.F.R. §3.71, the assignee hereby states that prosecution of the above-referenced patent application is to be conducted to the exclusion of the inventor(s).

Send all future correspondence to: Robert C. Kowert
Meyertons, Hood, Kivlin, Kowert &
Goetzel, P.C.

P.O. Box 398
Austin, Texas 78767-0398
(512) 853-8800

Assignee of Interest Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, California 95054

Dated: Oct. 12, 2006 By: Joseph A. Twarowski
Name: Joseph A. Twarowski
Reg. No.: 42,191
Title: Assistant General Counsel, IP Legal Group

APPENDIX A

Atty Dkt.	Client Ref.	Filing Date / Serial No.	Reel / Frame	Title	Inventors
6000-30301	P8147PSP	F 5/10/02 60/379,316	NA	Generic Implementation of Elliptic Curve Cryptography Using Partial Reduction	Hans Eberle Nils Gura
6000-30302	P8147PSP1	F 6/14/02 60/389,135	NA	Hardware Acceleration of Elliptic Curve Cryptography for Arbitrary Curves over GF(2m)	Nils Gura Hans Eberle
6000-30303	P8147PSP2	F 8/1/02 60/400,223	NA	End-to-End Systems Approach to Elliptic Curve Cryptography	Edouard Groupy, Hans Eberle Nils Gura
6000-30600	SUN050454PRV	F 8/17/05 60/708,928	NA	Conditional Multi-Store Synchronization Mechanisms	Mark Moir Robert Cypher Paul Lowenstein
6000-30602	SUN050454NP2	F 8/17/06 11/465,383	NA	Instruction Set Architecture Employing Conditional Multi-Store Synchronization	Mark Moir Robert Cypher Paul Lowenstein
6000-30700	SUN040362	F 7/20/04 10/894,829	015618 / 0987	Using Transactional Memory with Early Release to Implement Non-Blocking Dynamic-Sized Data Structure	Mark S. Moir Maurice Herlihy
6000-30800	SUN040363	F 7/20/04 10/894,828	015616 / 0710	Technique to Allow a First Transaction to Wait on Condition that Affects its Working Set	Mark S. Moir and Maurice Herlihy
6000-30900	SUN040496	F 12/30/04 11/026,255	015889 / 0294 & 016160 / 0569	Lightweight Reference Counting Using Single-Target Synchronization	Mark S. Moir, Simon Doherty, Victor M. Luchangco and Maurice Herlihy
6000-31000	SUN040495	F 9/14/05 11/226,038	016960 / 0400 & 016980 / 0660	Space-Adaptive Lock-Free Queue Using Pointer-Sized Single-Target Synchronization	Simon Doherty, Maurice Herlihy, Victor M. Luchangco and Mark S. Moir
6000-31100	SUN040488	F 12/30/04 11/026,849	015809 / 0312 & 016141 / 0814	Practical Implementation of Arbitrary-Sized LL/SC Variables	Mark S. Moir, Simon Doherty, Victor M. Luchangco and Maurice Herlihy
6000-31200	SUN040497	F 12/30/04 11/026,850	015832 / 0317 & 016141 / 0838	Space-Adaptive Lock-Free Free-List Using Pointer- Sized Single-Target Synchronization	Simon Doherty, Mark S. Moir, Simon Doherty, Victor M. Luchangco and Maurice Herlihy

6000-31300	SUN040584	F 4/23/04 10/830,661	015260 / 0290	Accelerating Elliptic Curve Point Multiplication Through Batched Inversions	Nils Gura, Stephen C. Fung, Douglas Stebila and Hans Eberle
6000-31400	SUN040649	F 11/23/04 10/995,885	015520 / 0813	Meta-Transactional Synchronization	Nir N. Shavit and Maurice P. Herlihy
6000-31401	SUN040649PSP	F 12/19/03 60/531,121	NA	Meta-Transactional Support for Synchronization	Nir N. Shavit and Maurice P. Herlihy
6000-31500	SUN030132	F 2/27/04 10/789,311	015038 / 0212	Method and Apparatus for Implementing Processor Instructions for Accelerating Public-Key Cryptography	Sheueling Chang Shantz, Leonard Rarick, Lawrence Spracklen, Hans Eberle and Nils Gura
6000-31600	SUN040665	F 8/10/04 10/915,502	015675 / 0605	Hybrid Software/Hardware Transactional Memory	Mark S. Moir
6000-31700	P8830	F 9/14/03 10/670,495	014547 / 0213	Efficient Non-Blocking K-Compare-Single-Swap Operation	Nir N. Shavit Mark S. Moir and Victor M. Luchangco
6000-31800	P2648	F 4/2/02 10/115,874 I 4/13/04 6,721,864	N/A	Programmable Memory Controller	Shrinath A. Keskar Massoud Hadjimohammadi
6000-31900	SUN050373	F 6/13/05 11/150,924	016709 / 0663	Dynamic Defense of Network Attacks	Radia J. Perlman
6000-32000	SUN040002	F 4/15/05 11/106,790	016483 / 0441	Obstruction-Free Data Structures and Mechanisms with Separable and/or Substitutable Contention Management Mechanisms	Mark S. Moir, Victor M. Luchangco and Maurice Herlihy
6000-32100	SUN050041	F 10/15/04 11/966,465	015906 / 0218	Scalable and Lock-Free First-In-First-Out Queue Implementation	Mark S. Moir, Orli Shalev and Nir N. Shavit
6000-32200	SUN050120	F 3/4/05 11/072,061	016366 / 0013	Method and Apparatus for Reducing Bandwidth Usage in Secure Transactions	Vipul Gupta, Nils Gura and Arvinderpal S. Wander
6000-32300	P9388PSP	F 6/30/2003 60/483,818	N/A	Accelerating Public-Key Cryptography	Sheueling CHang Shantz, Hans Eberle, Nils Gura, Lawrence Spracklen and Leonard Rarick
6000-32301	P9388	F 7/24/03 10/626,420	014320 / 0118	Method and Apparatus for Implementing Processor Instructions for Accelerating Public-Key Cryptography	Sheueling CHang Shantz, Hans Eberle, Nils Gura, Lawrence Spracklen and Leonard Rarick
6000-32400	P7125	F 1/10/03 10/340,156	014246 / 0325	Value Recycling Facility for Multithreaded Computations	Mark S. Moir, Victor Luchangco and Maurice Herlihy
6000-32401	P7125PSP	F 1/11/02 60/347,773	NA	Lock-Free Mechanism for Supporting Dynamic-Sized Data Structures, Implementations of the Lock-Free Mechanism and Exploitations Thereof for Exemplary	Mark S. Moir, Maurice Herlihy, Victor Luchangco,

				Classes of Data Structures and Software Development/Transformation Techniques	Paul A. Martin, David L. Detlefs, Guy L. Steele, Jr.
6000-32500	P8728	F 9/24/03 10/669,948	014547 / 0827	Quickly Reacquirable Locks	David Dice, Mark S. Moir and William N. Scherer, III
6000-32600	P8389	F 3/11/03 10/387,008	013866 / 0219	Generic Modular Multiplier Using Partial Reduction	Nils Gura and Hans Eberle
6000-32601	P8389PSP	F 11/15/02 60/426,783	NA	Cryptographic Processor for Arbitrary Elliptic Curves over GF(2m)	Hans Eberle, Nils Gura, Sheueling Change-Shantz
6000-32700	P8089	F 3/11/03 10/387,009	013866 / 0213	Modular Multiplier	Hans Eberle, Nils Gura, Russell A. Brown, Sheueling Change-Shantz and Vipul Gupta
6000-32800	SUN060319PSP	F 6/9/06 60/804,410	N/A	Systems and Methods for Debugging and Related Code Development Techniques Suitable for Transactional Memory	Yosef Lev, Mark S. Moir and Maurice P. Herlihy
6000-32900	SUN050178	F 6/20/05 11/156,822	016716 / 0937	Cluster-Wide Resource Usage Monitoring	Grzegorz J. Czajkowski, Glenn C. Skinner, Laurent P. Daynes and Krzysztof Palacz
6000-33000	P9203	F 1/10/03 10/340,150	013659 / 0780	Single-Word Lock-Free Reference Counting	Mark S. Moir, Victor Luchangco and Maurice Herlihy
6000-33100	SUN041115	F 12/9/04 11/008,692	016083 / 0271	Read Sharing for Transactional Memory	Yosef LEv and Mark S. Moir
6000-33200	P9630	F 2/20/04 10/783,738	015013 / 0834	Resource Management Interface	Grzegorz J. Czajkowski, Glenn C. Skinner, Ciaran J. Bryce, Stephen C. Hahn and Peter James Soper
6000-33300	P9631	F 2/20/04 10/783,448	015021 / 0003	Regulation of Resource Requests to Control Rate of Resource Consumption	Grzegorz J. Czajkowski, Glenn C. Skinner, Ciaran J. Bryce, Stephen C. Hahn and Peter James Soper
6000-33400	P9634	F 2/20/04 10/783,625	015014 / 0776	Resource Domains	Grzegorz J. Czajkowski, Glenn C. Skinner, Ciaran J. Bryce, Stephen C. Hahn and Peter James Soper
6000-33500	P7936	F 3/11/03 10/387,007	013870 / 0056	Hardware Accelerator for Elliptic Curve Cryptography	Hans Eberle, Nils Gura, Daniel Finchelstein, Sheueling Change-Shantz and Vipul Gupta

6000-33501	P7936PSP	F 5/1/02 60/376,742	NA	End-to-End System Approach to Elliptic Curve Cryptography	Hans Eberle, Nils Gura, Daniel F. Finchelstein, Chang Shantz, Sumit Gupta and Vipul Gupta
6000-33600	P8515	F 7/16/03 10/620,747	014298 / 0281	Obstruction-Free Mechanism for Atomic Update of Multiple Non-Contiguous Locations in Shared Memory	Mark S. Moir, Victor M. Luchangco and Maurice Herlihy
6000-33700	P8193	F 7/16/03 10/621,078	014304 / 0997	Space- and Time-Adaptive Nonblocking Algorithms	Mark S. Moir, Victor M. Luchangco and Maurice Herlihy
6000-33800	P8252	F 7/16/03 10/620,748	014299 / 0210	Obstruction-Free Synchronization for Shared Data Structures	Mark S. Moir, Victor M. Luchangco and Maurice Herlihy
6000-33900	SUN040206	F 6/11/04 10/866,570	014834 / 0714 & 014834 / 0645	Non-Blocking Growable Arrays	Mark S. Moir Simon Doherty
6000-34000	SUN050380	F 6/1/05 11/141,918	016365 / 0835	Method and Apparatus for Estimating Multithreaded Processor Throughput Based on Processor Cache Performance	Alexandra Fedorova
6000-34100	SUN030381	F 6/1/05 11/141,775	016349 / 0365	Method and Apparatus for Estimating the Effect of Processor Cache Memory Bus Delays on Multithreaded Processor Throughput	Alexandra Fedorova
6000-34200	SUN060067	F 12/19/05 11/311,506	017018 / 0933	Method and Apparatus for Improving Transaction Memory Interactions by Tracking Object Visibility	Yosef Lev Jan-Willem Maessen Mark S. Moir
6000-34300	SUN060361	F 8/29/06 11/511,804	NA	Method and Apparatus for Achieving Fair Cache Sharing on Multi-Threaded Chip Multiprocessors	Alexandra Fedorova
6000-34400	SUN040929PSP	F 3/2/04 60/549,238	NA	Comparing Elliptic Curve Cryptography and RSA on Small Devices	Nils Gura Lawrence A. Spracklen
6000-34401	SUN040929	F 11/23/04 10/996,103	015507/ 0453 & 016029 / 0832	Hybrid Multi-Precision Multiplication	Nils Gura Lawrence A. Spracklen
6000-34500	SUN040055	F 6/7/04 10/862,592	015457 / 0331	Accounting of Generationally Organized Memory	Grzegorz J. Czajkowski Glenn C. Skinner Laurent P. Daynes
6000-34600	SUN050180	F 5/10/05 11/125,579	016556 / 0227 &	Combining Different Resource Types	Grzegorz J. Czajkowski, Glenn C. Skinner Laurent P. Daynes
6000-35900	SUN060314	F 10/25/06 11/552,884	N/A	Breakpoints in a Transactional Memory-Based Representation of Code	Yosef Lev Mark S. Moir
6000-35800	SUN060315	F 10/25/06 11/552,895	N/A	Viewing and Modifying Transactional Variables	Yosef Lev Mark S. Moir Maurice P. Herlihy
6000-35700	SUN060316	F 10/25/06 11/552,890	N/A	Atomic Groups for Debugging	Yosef Lev Mark S. Moir

6000-35600	SUN060317	F 10/25/06 11/552,903	N/A	Watchpoints on Transactional Variables	Yosef Lev Mark S. Moir
6000-35500	SUN060318	F 10/25/06 11/552,907	N/A	Delayed Breakpoints	Yosef Lev Mark S. Moir
6000-31001	SUN040495CNT1	F 1/30/06 11/343,678	N/A	Code Preparation Technique Employing Lock-Free Pointer Operations	Mark S. Moir David L. Detlefs Simon Doherty Maurice P. Herlihy Victor M. Luchangco Paul A. Martin Guy L. Steele Jr.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND
DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

ME

004-30132

AUGUST 26, 2004

PTAS

ZAGORIN, O'BRIEN & GRAHAM, L.L.P.
MARK ZAGORIN
7600B N. CAPITAL OF TEXAS HWY, SUITE 350
AUSTIN, TX 78731



102687790A

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 02/27/2004

REEL/FRAME: 015038/0212
NUMBER OF PAGES: 5

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

SHANTZ, SHEUELING CHANG

DOC DATE: 02/26/2004

ASSIGNOR:

RARICK, LEONARD

DOC DATE: 02/25/2004

ASSIGNOR:

SPRACKLEN, LAWRENCE

DOC DATE: 02/25/2004

ASSIGNOR:

EBERLE, HANS

DOC DATE: 02/24/2004

ASSIGNOR:

GURA, NILS

DOC DATE: 02/26/2004

RECEIVED
ZAGORIN O'BRIEN & GRAHAM, L.L.P.

SEP 01 2004

015038/0212 PAGE 2

ASSIGNEE:

SUN MICROSYSTEMS, INC.
4150 NETWORK CIRCLE
SANTA CLARA, CALIFORNIA 95054

SERIAL NUMBER: 10789311

FILING DATE: 02/27/2004

PATENT NUMBER:

ISSUE DATE:

TITLE: METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR INSTRUCTIONS FOR
ACCELERATING PUBLIC-KEY CRYPTOGRAPHY

MARGARET LASALLE, PARALEGAL
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS

03-09-2004

ATTORNEY DOCKET NO.: 004-30132



ET

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

102687790

To the Honorable Commissioner of Patents and Trademarks. Please record the original documents or copy thereof.

1. Name of conveying party(ies):

Sheueling Chang Shantz; Leonard Rarick; Lawrence Spracklen;
Hans Eberle, and Nils Gura

Additional name(s) of conveying party(ies) attached?

☐ Yes ☒ No

2. Name and address of receiving party(ies):

Name: Sun Microsystems, Inc.

Internal Address: _____

Street Address: 4150 Network CircleCity/State/Zip: Santa Clara, CA 95054Additional name(s) & address(es) attached? ☐ Yes ☒ No

3. Nature of Conveyance:

- ☒ Assignment ☐ Merger
☐ Security Agreement ☐ Change of Name
☐ Other: _____

Execution Date(s): 2/26/04; 2/25/04; 2/25/04; 2/24/04; and
2/26/04, respectively

4. Application number(s) or patent number(s):

If this document is being filed together with a new application, the execution date of the application is: 2/26/04; 2/25/04;
2/25/04; 2/27/04; and 2/26/04, respectively

A. Patent Application No.:

B. Patent No.:

Additional numbers attached? ☐ Yes ☒ No

5. Name and address of party to whom correspondence concerning document should be mailed:

Name: Mark ZagorinInternal Address: Zagorin, O'Brien & Graham, L.L.P.Street Address: 7600B N. Capital of Texas Hwy, Suite 350City/State/Zip: Austin, TX 787316. Total number of applications and patents involved: 17. Total Fee (37 CFR 3.41): \$ 40.00

- ☒ A check is enclosed for the Total Fee shown above
☐ Please charge the Total Fee shown above to
Deposit Account 50-0631
☒ Authorized to charge additional fees to
Deposit Account 50-0631

03/04/2004 GWORDDF1 00000013 10789311

04 FC:8021

40.00 DP

DO NOT USE THIS SPACE

8. Statement and signature.

*To the best of my knowledge and belief, the foregoing information is true and correct and any attached copy is a true copy of the original document.*Mark Zagorin, 36,067
Name of Person SigningMark Zagorin
Signature2/27/04
DateTotal number of pages including cover sheet: 5

Express Mail Label No.: EV 401038618 US

ASSIGNMENT OF INVENTION

For good and valuable consideration, the receipt of which is hereby acknowledged,
I, an ASSIGNOR named below,

Sheueling Chang Shantz	of	Cupertino, CA
Leonard Rarick	of	Los Altos, CA
Lawrence Spracklen	of	Boulder Creek, CA
Hans Eberle	of	Mountain View, CA
Nils Gura	of	San Carlos, CA

hereby sell, assign and transfer to

ASSIGNEE: Sun Microsystems, Inc., a Delaware corporation, having a principal
place of business at 4150 Network Circle, Santa Clara, CA 95054,

its successors, assigns and legal representatives, my entire right, title and interest throughout
the world, including all rights to claim priority, in and to the invention(s) disclosed in:

- ☒ U.S. Patent Application executed on or about the date of this Assignment,
☐ U.S. Patent Application executed on _____, or
☐ U.S. Provisional Application
☐ U.S. Application No.: _____, filed on _____
☐ International Application No.: PCT/_____, filed on _____

ENTITLED: **METHOD AND APPARATUS FOR IMPLEMENTING
PROCESSOR INSTRUCTIONS FOR ACCELERATING
PUBLIC-KEY CRYPTOGRAPHY**, and naming as

INVENTOR(S): Sheueling Chang Shantz, Leonard Rarick, Lawrence Spracklen,
Hans Eberle, and Nils Gura

including without limitation, my entire right, title and interest in and to any and all United
States and foreign applications (including international, regional and foreign national
applications) for said invention(s), including divisions, continuations, continuations-in-part,
renewals, substitutes and extensions thereof, and in and to any and all patents of every
country or region that may be granted or have been granted for said invention(s), including
any reissues and reexaminations thereof.

To comply with 37 C.F.R. § 3.21 for recording this Assignment, I authorize and request that
the application number and filing date be inserted here, if not already shown above,
(_____/_____, filed _____) when they become known.

I authorize ASSIGNEE to apply for patents of foreign countries for said invention(s), and to
claim all rights of priority without further authorization from me.

I agree to execute any and all papers useful in connection with any and all United States and
foreign applications (including international, regional, and foreign national applications), and
generally to do everything possible to aid ASSIGNEE, its successors, assigns and nominees,
at their request and reasonable expense, in obtaining and enforcing patents for said
invention(s) in all countries.

ASSIGNMENT OF INVENTION

I hereby covenant that no assignment, sale, license, agreement, or encumbrance has been or will be made or entered into that would conflict with this Assignment.

I authorize and request the Commissioner of Patents and Trademarks to issue any U.S. Letters Patent that may be granted for said invention(s) to ASSIGNEE, its successors or assigns.

Executed on Feb 26, 2004 byShenling Chang Shantz
Shenling Chang Shantz

Executed on _____, 200__ by _____

Leonard Rarick

Executed on _____, 200__ by _____

Lawrence Spracklen

Executed on 2/24, 2004 byHans Eberle
Hans EberleExecuted on Feb 26, 2004 byNik Gura
Nik Gura

ASSIGNMENT OF INVENTION

For good and valuable consideration, the receipt of which is hereby acknowledged,
I, an ASSIGNOR named below,

Sheueling Chang Shantz	of	Cupertino, CA
Leonard Rarick	of	Los Altos, CA
Lawrence Spracklen	of	Boulder Creek, CA
Hans Eberle	of	Mountain View, CA
Nils Gura	of	San Carlos, CA

hereby sell, assign and transfer to

ASSIGNEE: Sun Microsystems, Inc., a Delaware corporation, having a principal
place of business at 4150 Network Circle, Santa Clara, CA 95054,

its successors, assigns and legal representatives, my entire right, title and interest throughout
the world, including all rights to claim priority, in and to the invention(s) disclosed in:

- ☒ U.S. Patent Application executed on or about the date of this Assignment,
☐ U.S. Patent Application executed on _____, or
☐ U.S. Provisional Application
☐ U.S. Application No.: _____, filed on _____
☐ International Application No.: PCT/_____, filed on _____

ENTITLED: **METHOD AND APPARATUS FOR IMPLEMENTING
PROCESSOR INSTRUCTIONS FOR ACCELERATING
PUBLIC-KEY CRYPTOGRAPHY**, and naming as

INVENTOR(S): Sheueling Chang Shantz, Leonard Rarick, Lawrence Spracklen,
Hans Eberle, and Nils Gura

including without limitation, my entire right, title and interest in and to any and all United
States and foreign applications (including international, regional and foreign national
applications) for said invention(s), including divisions, continuations, continuations-in-part,
renewals, substitutes and extensions thereof, and in and to any and all patents of every
country or region that may be granted or have been granted for said invention(s), including
any reissues and reexaminations thereof.

To comply with 37 C.F.R. § 3.21 for recording this Assignment, I authorize and request that
the application number and filing date be inserted here, if not already shown above,
(_____/_____, filed _____) when they become known.

I authorize ASSIGNEE to apply for patents of foreign countries for said invention(s), and to
claim all rights of priority without further authorization from me.

I agree to execute any and all papers useful in connection with any and all United States and
foreign applications (including international, regional, and foreign national applications), and
generally to do everything possible to aid ASSIGNEE, its successors, assigns and nominees,
at their request and reasonable expense, in obtaining and enforcing patents for said
invention(s) in all countries.

ASSIGNMENT OF INVENTION

I hereby covenant that no assignment, sale, license, agreement, or encumbrance has been or will be made or entered into that would conflict with this Assignment.

I authorize and request the Commissioner of Patents and Trademarks to issue any U.S. Letters Patent that may be granted for said invention(s) to ASSIGNEE, its successors or assigns.

Executed on _____, 200__ by _____
Sheueling Chang Shantz

Executed on February 25, 2004 by Leonard Rarick
Leonard Rarick

Executed on February 25, 2004 by [Signature]
Lawrence Spracklen

Executed on _____, 200__ by _____
Hans Eberle

Executed on _____, 200__ by _____
Nils Gura